Федеральное государственное бюджетное образовательное учреждение высшего образования «Петрозаводский государственный университет»

Отчёт

по лабораторной работе № 2 по курсу «Информационная безопасность и защита информации»

(Генерация псевдослучайных чисел)

Выполнил: студент 2 курса института математики и информационных технологий группы 22205 С. П. Гашков

Руководитель: В. Е. Соколов

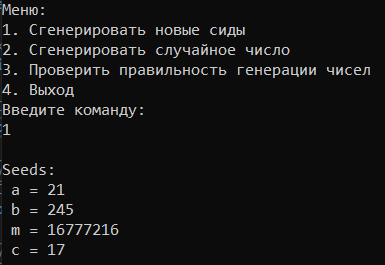
Петрозаводск

2022

Генератор псевдослучайных чисел (ГСПЧ) – метод, способный выдавать эмпирически-случайную последовательность чисел. На деле же этот метод позволяет последовательность чисел, которые даже в небольшом количестве, позволяют обеспечить относительную частоту, стремящуюся к нормальному распределению.

В данной работе реализован линейный конгруэнтный генератор. Он рекурсивен и зависим от трех параметров: чисел a,b и m и первого числа псевдослучайной последовательности. Данные числа, от которых зависит работа генератора, называется зерном(англ. seed, проф. «сид»).

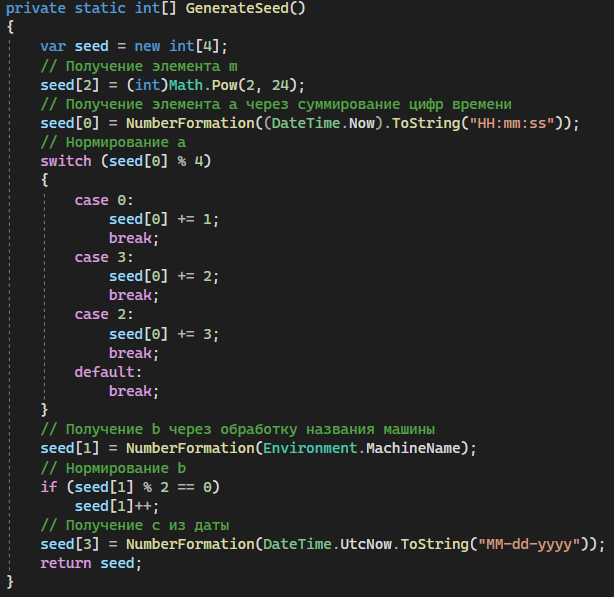
1. Генерация параметров ГСПЧ:



a, b – случайные числа, удовлетворяющих условиям

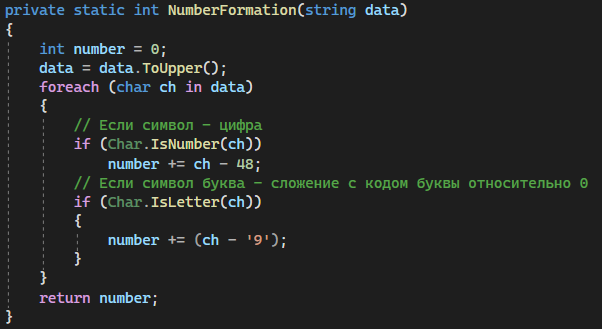
m – верхний предел сгенерированных чисел. В данной задаче задан равным 2^24

c – случайное число, являющееся первым в последовательности

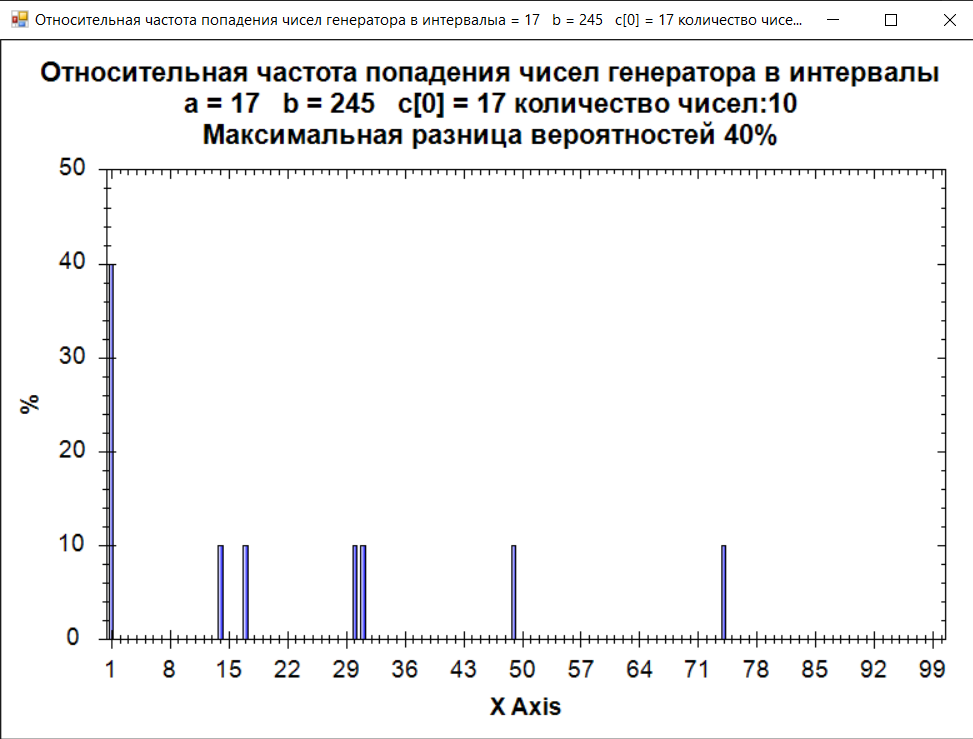


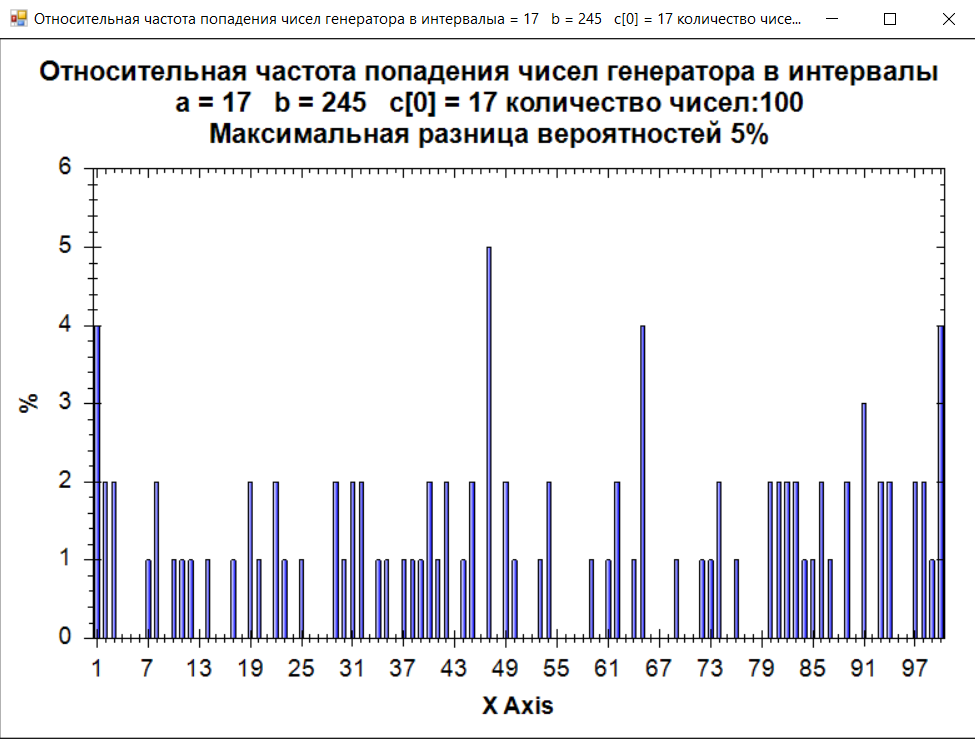
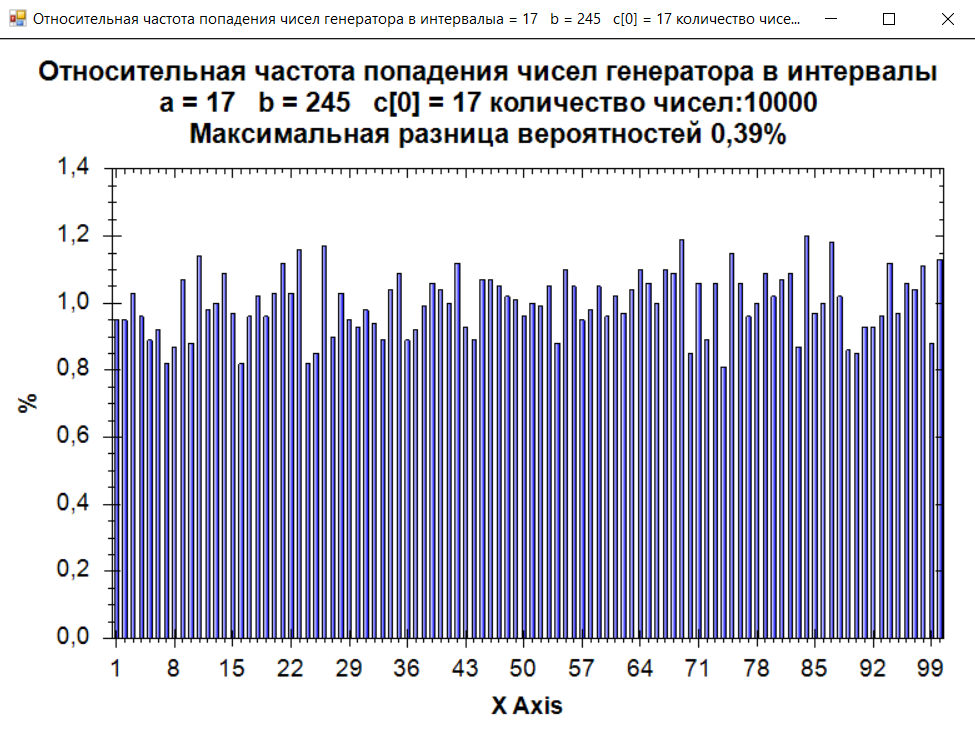
1. Получаем параметр m через возведение в степень
2. Получаем a через суммирование цифр времени
3. Приводим a к необходимому значению
4. Получаем b через обработку названия машины\*
5. Приводим b к необходимому значению
6. Получаем c через суммирование цифр даты
7. Выводим массив, содержащий сиды

\*Обработка строки случайных символов, возвращающее целое число:

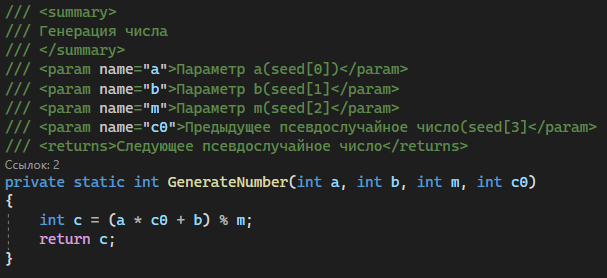


1. Перевод строки в нижний регистр
2. Если символ – цифра, то прибавляем её к сумме
3. Если символ – буква, то прибавляем к сумме её код относительно символа ‘9’ в кодировке ASCII
4. Возвращаем сумму
5. Статистика генерируемых чисел:



Начиная с 10000 сгенерированных чисел максимальная относительная разница в количестве чисел, разделенных на 100 равных интервалов, существенно меньше 1%. Соответственно, ГСПЧ производит ряд чисел, которые можно считать случайными, особенно на достаточно большом количестве чисел.

1. Функция генерации псевдослучайных чисел:



GenerateNumber принимает:

1. Параметр а (seed[0])
2. Параметр b (seed[1])
3. Параметр m (seed[2])
4. Предыдущее псевдослучайное число c0

Возвращает: целое c, являющееся следующим числом псевдослучайного ряда